UNIT - 3

Understanfing Ergonomics at Workplaces

Learning Outcomes

By the end of this unit the learner will be able to:

- ✓ Make your workplace a technology-friendly place
- ✓ Make the most of computers, telephones, instant messaging, e-mail, contact management applications, and scheduling software

Copyright©Staff Training Solutions, Ltd

Unit 3
Understanfing Ergonomics at Workplaces

What is Ergonomics?

Ergonomics is the study of using computers in a healthy manner to avoid hurting our bodies. Repetitive Strain Injuries (RSI) have increased, and so have employer's expenses as employees need time off work, medical treatment, and physiotherapy.

Things we must remember when using the computer include:

- ✓ Sit up straight with feet flat on the floor or on a footrest.
- ✓ Keep your lower arms level with the table and wrists straight.
- ✓ Always keep correct posture.
- ✓ Sit close enough to the keyboard to eliminate stretching but far enough away to avoid leaning.
- ✓ Tap the keys on your keyboard lightly.
- ✓ Place your mouse within easy reach of the hand you write with.
- ✓ Hold the mouse loosely. (You do not need to squeeze it.)
- ✓ The top of your monitor should line up with the top of your head.
- ✓ Take a short break every half hour or so. (You can stretch but do not disturb any other employees.)

Stretch!

STS
Staff Training Solutions

Head Turn

1. Slowly turn your head all the way to the left.
2. Pause.
3. Slowly turn your head all the way to the right.
4. Repeat process three times.

Shoulder Shrug

1. Relax shoulders.
2. Roll shoulders forwards, up to your ears, and then back down (to make a complete circle).
3. Repeat process three times forwards, three times backwards.

Arm Whirl

1. Make sure you are standing in a comfortable position with legs spread slightly apart.
2. Raise arms straight out until parallel with the floor.

Copyright©Staff Training Solutions, Ltd

3. Rotate arms, making ten large circles forward and ten circles backward.
4. Swing arms over head so that arms are perpendicular to ground. Hold for 20 seconds.
5. Lower arms and dangle below waist.

Tension Release

1. Sit on the floor and remove your shoes.
2. Start by wiggling your toes.
3. Kick legs three times.
4. Shake arms and head to finish the process.

Waking Up

1. While still sitting, close your eyes.
2. Yawn as wide as possible!
3. Open eyes.

System Usage Policies

What is a System Usage Policy?

A system usage policy is a contract between the employee and the employer detailing what the employee can and cannot do with the technology provided by the employer. Every organization, no matter how small, should have a policy in place. Be proactive: make sure everyone signs, reads, and understands the terms of use and why these policies are in place.

STS Staff Training Solutions

Topics that you should cover include:

- ✓ Appropriate Internet, software, e-mail and instant messaging usage
- ✓ If applications can be installed on company systems and what procedure must be followed to do so
- ✓ Employee's responsibilities regarding their systems (i.e. keep antivirus software up to date, don't open strange attachments, have strong passwords)
- ✓ What systems will be provided to the employee (cell phones, tablets, laptops, etc.) and what their responsibilities are with these systems
- ✓ What additional systems can be brought into the workplace (Some employers don't allow personal laptops or cell phones)
- ✓ Appropriate telephone usage (Are any personal calls allowed? Are long distance calls allowed?)
- ✓ No food and drink near electronics (cell phones, laptops, tablets, keyboards)
- ✓ Employee has no expectation of privacy when using company systems (meaning instant messaging, Internet surfing, e-mail, and phone conversations can all be monitored)
- ✓ Policy can be revised at any time (also explain how employees will be notified)
- ✓ What the consequences will be if policy is not adhered to
- ✓ Who to contact with system issues

Copyright©Staff Training Solutions, Ltd

Your system usage policy should reflect the organization. If you're a small company with only three employees, a short policy based on the honor system should be fine. If you're a larger company, then you need a larger policy. You should also make plans to periodically review the policy with either your internal system administrator or an external expert.
Remember, the policy needs to be enforced to have any weight. Consequences for breaching the policy should be outlined in it. Supervisors must have the weight to both monitor the conditions outlined in the policy and discipline staff as necessary. If changes are made to the policy, each supervisor should review the changes with their team and have each member re-sign the policy.

Sample Internet, E-Mail, and Computer Usage Policy

Policy Statement
The use of XYZ Company (Company) automation systems, including computers, fax machines, and all forms of Internet/Intranet access, is for company business and for authorized purposes only. Brief and occasional personal use of the electronic mail system or the Internet is acceptable as long as it is not excessive or inappropriate, occurs during personal time (lunch or other breaks), and does not result in expense to the Company.

Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities. Electronic communication should not be used to solicit or sell products or services that are unrelated to the Company's business; distract, intimidate, or harass coworkers or third parties; or disrupt the workplace.

Use of Company computers, networks, and Internet access is a privilege granted by management and may be revoked at any time for inappropriate conduct carried out on such systems, including, but not limited to:

Sending chain letters or participating in any way in the creation or transmission of unsolicited commercial e-mail ("spam") that is unrelated to legitimate Company purposes;

Engaging in private or personal business activities, including excessive use of instant messaging and chat rooms (see below);

Misrepresenting oneself or the Company;

Violating the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way;

Engaging in unlawful or malicious activities;

Copyright©Staff Training Solutions, Ltd

Deliberately propagating any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the Company's networks or systems or those of any other individual or entity;

Using abusive, profane, threatening, racist, sexist, or otherwise objectionable language in either public or private messages;

Sending, receiving, or accessing pornographic materials;

Becoming involved in partisan politics;
Causing congestion, disruption, disablement, alteration, or impairment of Company networks or systems;

Maintaining, organizing, or participating in non-work-related Web logs ("blogs"), Web journals, "chat rooms," or private/personal/instant messaging;

Failing to log off any secure, controlled-access computer or other form of electronic data system to which you are assigned, if you leave such computer or system unattended;

Using recreational games; and/or

Defeating or attempting to defeat security restrictions on company systems and applications.

Using Company automation systems to access, create, view, transmit, or receive racist, sexist, threatening, or otherwise objectionable or illegal material is strictly prohibited. "Material" is defined as any visual, textual, or auditory entity. Such material violates the Company anti-harassment policies and is subject to disciplinary action. The Company's electronic mail system, Internet access, and computer systems must not be used to violate the laws and regulations of the United States or any other nation or any state, city, province, or other local jurisdiction in any way. Use of company resources for illegal activity can lead to disciplinary action, up to and including dismissal and criminal prosecution. The Company will comply with reasonable requests from law enforcement and regulatory agencies for logs, diaries, archives, or files on individual Internet activities, e-mail use, and/or computer use.

Unless specifically granted in this policy, any non-business use of the Company's automation systems is expressly forbidden.

If you violate these policies, you could be subject to disciplinary action, up to and including dismissal.

Ownership and Access of Electronic Mail, Internet Access, and Computer Files

Copyright©Staff Training Solutions, Ltd

The Company owns the rights to all data and files in any computer, network, or other information system used in the Company. The Company also reserves the right to monitor electronic mail messages (including personal/private/instant messaging systems) and their content, as well as any and all use of the Internet and of computer equipment used to create, view, or access e-mail and Internet content. Employees must be aware that the electronic mail messages sent and received using Company equipment are not private and are subject to viewing, downloading, inspection, release, and archiving by Company officials at all times. The Company has the right to inspect any and all files stored in private areas of the network or on individual computers or storage media in order to assure compliance with policy and state and federal laws. No employee may access another employee's computer, computer files, or electronic mail messages without prior authorization from either the employee or an appropriate Company official.

The Company has licensed the use of certain commercial software application programs for business purposes. Third parties retain the ownership and distribution rights to such software. No employee may create, use, or distribute copies of such software that are not in compliance with the license agreements for the software. Violation of this policy can lead to disciplinary action, up to and including dismissal.

Confidentiality of Electronic Mail

As noted above, electronic mail is subject at all times to monitoring, and the release of specific information is subject to applicable state and federal laws and Company rules, policies, and procedures on confidentiality. Existing rules, policies, and procedures governing the sharing of confidential information also apply to the sharing of information via commercial software. Since there is the possibility that any message could be shared with or without your permission or knowledge, the best rule to follow in the use of electronic mail for non-work-related information is to decide if you would post the information on the office bulletin board with your signature.

It is a violation of Company policy for any employee, including system administrators and supervisors, to access electronic mail and computer systems files to satisfy curiosity about the affairs of others. Employees found to have engaged in such activities will be subject to disciplinary action.

Electronic Mail Tampering

Electronic mail messages received should not be altered without the sender's permission; nor should electronic mail be altered and forwarded to another user and/or unauthorized attachments be placed on another's electronic mail message.

Policy Statement for Internet/Intranet Browser(s)

The Internet is to be used to further the Company's mission, to provide effective service of the highest quality to the Company's customers and staff, and to support other direct job-related purposes. Supervisors should work with employees to determine the appropriateness of using the Internet for

Copyright©Staff Training Solutions, Ltd

professional activities and career development. The various modes of Internet/Intranet access are Company resources and are provided as business tools to employees who may use them for research, professional development, and work-related communications. Limited personal use of Internet resources is a special exception to the general prohibition against the personal use of computer equipment and software.

Employees are individually liable for any and all damages incurred as a result of violating company security policy, copyright, and licensing agreements.

All Company policies and procedures apply to employees' conduct on the Internet, especially, but not exclusively, relating to: intellectual property, confidentiality, company information dissemination, standards of conduct, misuse of company resources, anti-harassment, and information and data security.

Personal Electronic Equipment

The Company prohibits the use or possession in the workplace of any type of camera phone, cell phone camera, digital camera, video camera, or other form of image-recording device without the express permission of the Company and of each person whose image is recorded. Employees with such devices should leave them at home unless expressly permitted by the Company to do otherwise. This provision does not apply to designated Company personnel who must use such devices in connection with their positions of employment.

Employees should not bring personal computers to the workplace or connect them to Company electronic systems unless expressly permitted to do so by the Company. Any employee bringing a personal computing device or personal imaging device onto Company premises thereby gives permission to the Company to inspect the personal computer at any time with personnel of the Company's choosing and to analyze any files, other data, or data storage media that may be within or connectable to the personal computer in question. Employees who do not wish such inspections to be done on their personal computers or imaging devices should not bring such items to work at all.

Policy Enforcement

Violation of this policy, or failure to permit an inspection of any device covered by this policy, shall result in disciplinary action, up to and possibly including immediate termination of employment. In addition, the employee may face both civil and criminal liability from the Company or from individuals whose rights are harmed by the violation.

Employee Signature: _____

Date: _____

Acme Consulting, Part Three

Copyright©Staff Training Solutions, Ltd

The folks that we consulted for yesterday have taken our advice, thought about it, and come up with solutions to their technical problems. Now they want our help in writing a system usage policy.

Scenario One

Fifty-two year old Tom Pipes runs a plumbing business that has been in the family for decades. After his discussion with Acme Consulting, he decided to purchase a computer for his office and get some training. He now uses Microsoft Outlook to track his appointments. Each of his plumbers has a smartphone that syncs with the main computer every morning. They also have cell phones to help keep them connected with the office.

Create the basic outline for a system usage policy.

Scenario Two

Mark Monson owns and runs a small advertising firm. His staff of six has struggled long and hard through the first few years of business. Now that they're turning a profit, he treated them all to new computer systems and software that can make designing ads a lot easier. He's also connected all the systems to a domain and hired a system administrator.

Software that the staff uses includes:

- ✓ Word Plus (a word processing program)
- ✓ Ad Plus (a design program)

Copyright©Staff Training Solutions, Ltd

- ✓ Photo Plus (an image processing program)
- ✓ Messages Plus (an e-mail program)
- ✓ Internet Explorer

Of course, his employees each have an office-based phone that they can use. Cell phones are not provided by the company.

Create the basic outline for a system usage policy.

Scenario Three

After much discussion with a consulting team, the CEO of Acme Consulting has decided to purchase mobile tools (smartphones and tablets) for the consulting staff. She wants to have a system usage policy in place that will be issued with the tools.

Create the basic outline for a system usage policy.

Copyright©Staff Training Solutions, Ltd

Scenario Four

During her struggle to find the perfect manager, Lisa Leeds has realized that her whole company needs some help dealing with technology. All employees have a phone and fax machine in their cube. As well, all staff have a desktop computer connected to a router.

STS Staff Training Solutions

Software they use includes:

- ✓ Word Plus (a word processing program)
- ✓ Numbers Plus (a spreadsheet program)
- ✓ Time Plus (a scheduling program)
- ✓ Messages Plus (an e-mail program)
- ✓ Internet Explorer
- ✓ Windows Messenger (an instant messaging program)

Create the basic outline for a system usage policy.

Copyright©Staff Training Solutions, Ltd

Taking Care of Company Property

Basic Rules of Etiquette
Laptops, tablets, and cell phones have become essential tools, especially for business travelers. Sometimes, companies will provide these tools to take off-site.

The Manager's Role
If you're the manager, set expectations about proper use of the device. When and where will it be used? As well, deal with financial issues before they arise. For a cell phone, if there are extra charges, who will pay? Or if the device is broken, who will pay? (Note that usually it's the employer who is responsible for repairs.)

You will also want to make sure that devices are tracked properly. If no company standard is in place, you may want to set up a simple table listing the device name, serial number, phone number (if applicable), what condition it was when it was issued, and the date that it was issued. If repairs are your responsibility, make sure you keep good records.

The Employee's Role
If you're the employee, there's some good news! This responsibility means a bit more flexibility. For example, I have colleague who works from home. Her personal computer has games and music on it as well as her work, as it's her own system. However, her company purchased her a laptop, and this only has work applications on it: no games, and only classical music to help her concentrate. However, when she travels, she does use it to check her personal e-mail on her own time. You must be respectful of these perks at all times; after all, is still someone else's property.

Even if you don't travel, you still use company property at work, whether it's a computer, a coffee maker, a fax machine, a printer, or a telephone. The key thing to remember about these devices is that it's all someone else's property and that you are being allowed to use it. Never, ever leave something broken. If you arrive at the printer and it's jammed, you should try to fix it. If you can't fix it or don't have time, leave a sign on it that says it's out of order and let someone who can fix it know about the problem. It's just common courtesy.

Copyright©Staff Training Solutions, Ltd

Role Play
List of Scenarios

- ✓ An employee left the coffee pot on with no coffee in it. The pot broke and another employee stepped on the glass and was injured.
- ✓ You have borrowed your manager's cell phone for an out-of-town meeting. You notice that there are some personal pictures on the phone.
- ✓ You've just gotten the cell phone bill for one of your staff members. There are some long distance charges on there and you're not sure if they're work-related or not.
- ✓ An employee is trying to print an important document but someone has left the printer jammed. S/he has a suspicion about who it is, and it's not the first time this has happened.
- ✓ Employee A has come to you about Employee B making personal calls at work. Employee A says that Employee B is constantly on the phone and speaks loudly about personal issues. This distracts other employees and causes awkwardness as everyone knows about this employee's personal life. How do you deal with Employee B?
- ✓ You've noticed that one of your staff members is in the washroom an awful lot and that s/he brings their personal cell phone with them.
- ✓ The employer has been kind enough to provide a computer with Internet access in the staff break room. However, one employee monopolizes the computer to work on their resume and hunt for a new job.

Outline your role play in the space below.

STS
Staff Training Solutions

Further Reading: